Matematyka dyskretna

© Andrzej Łachwa, UJ, 2019
andrzej.lachwa@uj.edu.pl

6/14

Podzielność

Niech liczba całkowita $p>0$. Dla każdej liczby całkowitej a mówimy, że ***a* jest podzielna przez *p*** (p jest dzielnikiem a, p dzieli a, $p|a$), jeśli istnieje liczba całkowita q taka, że $a=pq$.

Dla dowolnych całkowitych a, b, c zachodzi:
jeśli $a|b$ to $a|bc$,
jeśli $a|b$ i $b|c$ to $a|c$,
jeśli $a|b$ i $a|c$ to $a|(b+c)$.

Dowolną liczbę wymierną a można wydzielić przez dowolną niezerową liczbę wymierną b i wynik tego działania jest liczbą wymierną.

Niech liczba całkowita $p>0$. Wtedy dla każdej liczby całkowitej a istnieją jednoznacznie wyznaczone: **iloraz** q i **reszta** r spełniające

$$a = pq + r \quad \text{oraz} \quad 0 \leq r < p.$$

Resztę r z dzielenia a przez p zapisujemy też jako: ***a* mod *p***.
Iloraz q zapisujemy jako: ***a* div *p***.

$$a \text{ div } p = \lfloor a/p \rfloor$$
$$a \text{ mod } p = a - p \cdot (a \text{ div } p)$$

Wartości funkcji „mod p” znajdują się w zbiorze $\{0, 1, 2, \ldots p\text{-}1\} = Z_P$.
Funkcja ta przekształca zbiór Z na zbiór Z_P.

Przykłady
31 mod 5 = 1, (-31) mod 5 = 4, 31 div 5 = 6, (-31) div 5 = -7

Twierdzenie

$[a^{b+c}]_p \equiv [\,[a^b]_p \cdot [a^c]_p\,]_p$

Zadanie 1

Oblicz 10^{39} mod 11.

Twierdzenie

Jeżeli $[a]_m \equiv [b]_m$ i $[c]_m \equiv [d]_m$

to $[a+c]_m \equiv [b+d]_m$, $[a-c]_m \equiv [b-d]_m$, $[a \cdot c]_m \equiv [b \cdot d]_m$

Zadanie 2

Oblicz (50·51+15) mod 7.

Rozw. zad. 1

$10^1 \bmod 11 = 10$

$10^2 \bmod 11 = 1$

$10^4 \bmod 11 = 1$ bo $[10^{2+2}]_{11} \equiv [\,[10^2]_{11} \cdot [10^2]_{11}\,]_{11} \equiv [\,1 \cdot 1\,]_{11} \equiv [\,1\,]_{11}$

$10^8 \bmod 11 = 1$ bo $[10^{4+4}]_{11} \equiv [\,[10^4]_{11} \cdot [10^4]_{11}\,]_{11} \equiv [\,1 \cdot 1\,]_{11} \equiv [\,1\,]_{11}$

$10^{16} \bmod 11 = 1$

$10^{32} \bmod 11 = 1$

$10^{39} = 10^{32+4+2+1}$ więc

$[10^{39}]_{11} \equiv [\,1 \cdot 1 \cdot 1 \cdot 10]_{11} \equiv [\,10\,]_{11}$

zatem $10^{39} \bmod 11 = 10$

Rozw. zad. 2

$[50]_7 \equiv [1]_7$, $[51]_7 \equiv [2]_7$, $[15]_7 \equiv [1]_7$

więc

$[50 \cdot 51+15]_7 \equiv [1 \cdot 2+1]_7 \equiv [3]_7$

zatem

$(50 \cdot 51+15) \bmod 7 = 3$

NWD

Największy wspólny dzielnik NWD(a, b) liczb a i b, gdzie chociaż jedna z tych liczb jest różna od 0, to największa liczba d taka, że $d|a$ i $d|b$.

Oczywiście, $1 \leq \text{NWD}(a, b) \leq \min(a, b)$.

Algorytm Euklidesa

(1) Wczytaj liczby a, b >0.
(2) Oblicz r jako resztę z dzielenia a przez b.
(3) Zastąp a przez b, zaś b przez r.
(4) Jeżeli b=0 to zwróć a w przeciwnym wypadku przejdź do (2).

Przykład

$$
\begin{array}{llll}
a = 1029 & b = 1071 & 1029 = 0 \cdot 1071 + 1029 & r = 1029 \\
a = 1071 & b = 1029 & 1071 = 1 \cdot 1029 + 42 & r = 42 \\
a = 1029 & b = 42 & 1029 = 24 \cdot 42 + 21 & r = 21 \\
a = 42 & b = 21 & 42 = 2 \cdot 21 + 0 & r = 0 \\
a = 21 & b = 0 & &
\end{array}
$$

NWD(1029, 1071) = 21

Dla dowodu poprawności algorytmu Euklidesa ustalmy dwie liczby naturalne $a > b > 0$. Jeśli $a < b$ to podany algorytm odwróci ich porządek przy pierwszym wykonaniu kroku (3). Zauważmy, że w każdym następnym kroku $a > b > r$ ponieważ reszta z dzielenia a przez b leży w zbiorze $\{0, \ldots, b-1\}$. A zatem kolejne reszty będą tworzyć ciąg ściśle malejący, który w końcu osiągnie 0, czyli algorytm Euklidesa po pewnej skończonej ilości kroków się zatrzyma.

Pozostaje sprawdzić, czy algorytm Euklidesa zwraca właściwą odpowiedź. Niech $r = a \bmod b$, tzn. $r = a - bq$ dla pewnego q. Wszystkie dzielniki a i b dzielą prawą stronę ostatniej równości, a więc dzielą też r, co implikuje $\mathrm{NWD}(a, b) = \mathrm{NWD}(b, r)$. Dowodzi to, iż wszystkie pary rozważane przez algorytm mają te same dzielniki, a więc ten sam NWD…

Rozszerzenie algorytmu Euklidesa

Algorytm Euklidesa można zastosować do wskazania dwu dodatkowych liczb całkowitych *x*, *y* takich, że

$$ax + by = \mathrm{NWD}(a, b).$$

Fakt ten leży u podstaw wielu twierdzeń, jest stosowany do rozwiązywania równań i w przekształceniach kryptograficznych.

Dowód

Załóżmy, że $a>b$. Niech $r_0 = a$, $r_1 = b$, natomiast $r_2 \cdots, r_n, r_{n+1}$ będą kolejnymi resztami wygenerowanymi przez algorytm Euklidesa, oraz $r_{n+1} = 0$ i wtedy $r_n = \mathrm{NWD}(a, b)$.

Dla każdej reszty r_{i+2} istnieje pewne q_{i+1} takie, że $r_{i+2} = r_i - q_{i+1} \cdot r_{i+1}$.

Indukcyjnie dowodzimy:

(1) $r_2 = r_0 - q_1 r_1 = a - q_1 b$ czyli $x=1$, $y=-q_1$

(2) zakładamy, że dla każdego j=2, 3 …, i+1 jest istnieją *x*, *y* takie, że $r_j=xa+yb$ i liczmy $r_{i+2} = r_i - q_i r_{i+1} = r_i - q_i (r_{i-1} - q_{i-1} r_i) = r_i(1 - q_{i-1}) - q_i r_{i-1}$

$= (ax'+by')(1-q_{i-1}) - q_i (ax''+by'') = a(x'-x'q_{i-1} - q_i x'') + b(y'-y'q_{i-1} - q_i y'')$

A zatem dla r_n = NWD(*a*,*b*) też istnieją odpowiednie *x*, *y*.

Czas działania algorytmu

Niech $r_0, r_1, \ldots, r_{n+1}$ będą zdefiniowane, jak w dowodzie powyżej. Załóżmy dodatkowo, iż $a > b$ (jeśli nie, to zaczynamy analizować po pierwszym kroku algorytmu). Pokażemy, że $r_{j+2} < \frac{1}{2} r_j$.

Jeśli $r_{j+1} \leq \frac{1}{2} r_j$, to natychmiast mamy $r_{j+2} < r_{j+1} \leqslant \frac{1}{2} r_j$. Załóżmy więc, że $r_{j+1} > \frac{1}{2} r_j$. W tym przypadku podczas dzielenia r_j przez r_{j+1} zachodzi $r_j = 1 \cdot r_{j+1} + r_{j+2}$, czyli $r_{j+2} = r_j - r_{j+1} < \frac{1}{2} r_j$.

Ponieważ po każdych, kolejnych dwu krokach rozmiar r_j spada co najmniej dwukrotnie, kroków jest $O(\lg a)$. W każdym kroku przeprowadzane jest dzielenie liczb długości $O(\lg a)$, a więc $O(\lg^2 a)$ operacji bitowych. To oznacza, iż do policzenia $\mathrm{NWD}(a, b)$ ($a \geq b$) algorytmem Euklidesa wystarcza $O(\lg^3 a)$ operacji bitowych.

Aby policzyć współczynniki *x*, *y* takie, że $ax + by = \mathrm{NWD}(a, b)$, zgodnie z przedstawionym dowodem, należy przedstawić $\mathrm{NWD}(a, b)$ jako kombinację r_{n-1} i r_{n-2}, a później pozbyć się kolejnych r_i (poczynając od r_{n-1}) wprowadzając r_{i-2}. Mamy więc $O(\lg a)$ kroków i w każdym kroku przeprowadzamy mnożenie i dodawanie lub odejmowanie liczb o długości co najwyżej $O(\lg a)$. Mamy zatem $O(\lg^2 a)$ operacji bitowych.

Przykład dla $a = 1547$ i $b = 560$.

$$1547 = 2 \cdot 560 + 427$$
$$560 = 1 \cdot 427 + 133$$
$$427 = 3 \cdot 133 + 28$$
$$133 = 4 \cdot 28 + 21$$
$$28 = 1 \cdot 21 + 7$$
$$21 = 3 \cdot 7 + 0.$$

A więc $\mathrm{NWD}(1547, 560) = 7$.

Aby wyrazić 7 jako kombinację danych wejściowych liczymy:

$$
\begin{aligned}
7 &= \mathbf{28} - 1 \cdot \mathbf{21} = 28 - 1 \cdot (133 - 4 \cdot 28) \\
&= -1 \cdot \mathbf{133} + 5 \cdot \mathbf{28} = -1 \cdot 133 + 5 \cdot (427 - 3 \cdot 133) \\
&= 5 \cdot \mathbf{427} - 16 \cdot \mathbf{133} = 5 \cdot 427 - 16 \cdot (560 - 1 \cdot 427) \\
&= -16 \cdot \mathbf{560} + 21 \cdot \mathbf{427} = -16 \cdot 560 + 21 \cdot (1547 - 2 \cdot 560) \\
&= 21 \cdot \mathbf{1547} - 58 \cdot \mathbf{560}.
\end{aligned}
$$

Liczby pierwsze

Ze wstępu do książki E. Gracjana: „… liczby pierwsze to niesforna zgraja. Pojawiają się tam gdzie chcą, bez ostrzeżenia, w sposób pozornie chaotyczny, bez żadnych reguł. A najgorsze, że nie da się ich ignorować – są absolutnie niezbędne …”

Liczba naturalna jest nazywana pierwszą gdy jest podzielna tylko przez 1 i przez samą siebie, tzn. gdy posiada dokładnie dwa różne dzielniki.

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Liczba złożona to liczba naturalna, która nie jest pierwsza, a więc ma jakiś dodatni dzielnik różny od 1 i od niej samej. Pozostają liczby 0 i 1!

Fundamentalne twierdzenie arytmetyki

Każdą liczbę naturalna można zapisać jako iloczyn liczb pierwszych i na dodatek taki rozkład na czynniki pierwsze jest tylko jeden (z dokładnością do kolejności czynników).

Liczby pierwsze służą więc do utworzenia wszystkich innych liczb!

120	2
60	2
30	2
15	3
5	5
1	

Zatem $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$

Skąd wziąć kolejne liczby pierwsze do powyższego dzielenia?

Obecnie nie jest znany żaden **efektywny algorytm faktoryzujący** liczby naturalne, tzn. znajdujący rozkład na iloczyn liczb pierwszych. Oczekiwana trudność tego problemu jest sercem wielu współczesnych systemów kryptograficznych (np. RSA).

Nie wszystkie liczby są równie trudne w rozkładzie. Póki co, (w połowie 2006 roku) najtrudniejsze wydają się liczby, które są iloczynami dwu liczb pierwszych podobnej długości.

Aby choć trochę zrozumieć trudność problemu faktoryzacji proponujemy znaleźć nietrywialny dzielnik liczby złożonej 10721. Na stronie WWW firmy RSA podane są znacznie większe liczby, za rozkład których RSA skłonna jest płacić nawet 200 tys. USD.

Sito Eratostenesa

Jak wyznaczyć wszystkie liczby pierwsze niewiększe od *n*?

Jeszcze w czasach starożytnych Eratostenes opisał metodę postępowania rozwiązującą ten problem dla małych *n*. Oto ten algorytm:

(1) Wczytaj *n*. Wypisz listę wszystkich liczb naturalnych od 2 do *n*. Na początku wszystkie liczby są nieskreślone.

(2) Dopóki istnieje nieskreślona jeszcze liczba na naszej liście niewiększa od $\sqrt{n}$ powtarzaj:

> (*) Weź pierwszą nieskreśloną liczbę *p* z listy i dodaj do zbioru znalezionych liczb pierwszych. Później skreśl liczbę *p* z listy i skreśl wszystkie wielokrotności liczby *p*, które są jeszcze na liście.

(3) Wszystkie pozostałe nieskreślone liczby z listy dodaj do zbioru znalezionych liczb pierwszych.

Przykłady

Dla n=100 skreślanie opisane w (*) wykonamy cztery razy, kolejno dla liczb pierwszych 2, 3, 5 i 7 (bo następna liczba pierwsza, czyli 11, jest już większa od pierwiastka ze 100). Sito zostawi 25 liczb pierwszych, w tym 21 liczb większych od 10.

Dla n=400 skreślanie wykonamy osiem razy (dla kolejnych ośmiu liczb pierwszych, bo dziewiąta liczba pierwsza jest większa od pierwiastka z 400). Sito zostawi 78 liczb pierwszych, w tym 70 liczb większych od 20.

Dla n=10 000 skreślanie wykonamy 25 razy, a sito zostawi 1229 liczb pierwszych, w tym 1204 liczby z przedziału (100, 10 000).

Jak rozłożone są liczby pierwsze? Jak długie są przerwy między kolejnymi liczbami pierwszymi?

Dziwne, ale są dowolnie długie!

Dla przykładu:

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5+2$

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5+3$

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5+4$

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5+5$ to cztery kolejne liczby naturalne, które nie są pierwsze.
Aby uzyskać 100 kolejnych liczb naturalnych, w których nie występuje liczba pierwsza, weźmy: $101!+2$, $101!+3$, … $101!+101$

Można więc skonstruować dowolnie długi ciąg liczb naturalnych,
w którym nie występuje ani jedna liczba pierwsza.

Ile jest liczb pierwszych?

Euklides pokazał, że nieskończenie wiele.

Dla dowodu weźmy dowolną listę początkowych liczb pierwszych, np. 2, 3, 5, 7, 11, 13. Tworzymy nową liczbę jako następnik iloczynu tychże liczb pierwszych:

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$$

Taka liczba nie jest podzielna przez żadną z liczb pierwszych z naszej listy (bo zawsze dzielenie da resztę 1). Liczba ta może być pierwsza, ale może być złożona. Jeżeli jest to liczba pierwsza, to znaczy, że jest większa od liczb z naszej listy. Jeżeli jest to liczba złożona (w naszym przykładzie $30031 = 59 \cdot 509$), to znaczy, że ma rozkład na liczby pierwsze większe od liczb z naszej listy. W obu przypadkach dla dowolnie długiej listy liczb pierwszych wykazano istnienie liczby pierwszej większej od liczb z tej listy.

Liczby doskonałe

Rozważmy wszystkie dzielniki liczby mniejsze od tej liczby.

Mówimy, że liczba jest nadmiarowa, gdy suma jej dzielników jest od niej większa. Niedomiarowa – gdy suma jej dzielników jest od niej mniejsza.

Liczba 30 jest nadmiarowa, bo suma jej dzielników 1+2+3+5+6+10+15=42 i jest od niej większa. Liczba 25 jest niedomiarowa, bo suma jej dzielników wynosi 1+5=6 i jest od niej mniejsza. Każda liczba pierwsza jest bardzo niedomiarowa, bo suma jej dzielników wynosi 1.

Liczba doskonała to taka, która nie jest ani nadmiarowa, ani niedomiarowa.

Początkowe liczby doskonałe:

6, 28, 496, 8 128, 33 550 336, 8 589 869 056, 137 438 691 328.

Nie wiadomo, czy zbiór tych liczb jest skończony, czy nie!

Liczby względnie pierwsze

Liczby *a*, *b* są względnie pierwsze wtw gdy $\mathrm{NWD}(a,b)=1$, co zapisujemy inaczej jako $a \perp b$. Na przykład $10 \perp 3$.

Elementy Euklidesa zawierają słynny lemat:

Jeśli $n \mid ab$ i $n \perp a$, to $n \mid b$.

Dowód

Ponieważ $\mathrm{NWD}(a,n)=1$, to istnieją całkowite *x*, *y* takie, że $xa+yn=1$.

Mnożąc obie strony równości przez *b* otrzymujemy $xab+ynb=b$.

Z założenia wiemy, iż *n* dzieli lewą stronę powyższej równości (dokładnie mówiąc: dzieli lewy składnik sumy). Musi zatem dzielić też prawą.

Każdą liczbę $n>1$ można przedstawić jako iloczyn liczb pierwszych.

Dowód

Intuicyjnie, wystarczy rozkładać liczby złożone na iloczyn, aż wszystkie liczby w tym iloczynie będą liczbami pierwszymi.

Dla formalnego dowodu załóżmy niewprost, iż istnieje liczba naturalna większa od 1, nierozkładalna na iloczyn liczb pierwszych. Korzystając z Zasady Minimum, weźmy najmniejszą taką liczbę n. Musi to być liczba złożona, gdyż dowolna liczba pierwsza jest jednoelementowym iloczynem liczb pierwszych. A zatem n jest złożona i istnieją a, $b > 1$ takie, że $n=ab$. Ale wtedy a oraz b są mniejsze od n, więc z minimalności n, rozkładają się na iloczyn liczb pierwszych. Ale wtedy także $n=ab$ byłoby iloczynem liczb pierwszych, co przeczy temu, że n jest nierozkładalna na iloczyn liczb pierwszych i kończy dowód.

Dowód fundamentalnego twierdzenia arytmetyki

Najpierw przedstawimy dowód pochodzący od Euklidesa. Niech $n > 1$ będzie najmniejszą liczbą naturalną posiadającą dwa różne rozkłady na liczby pierwsze: $p_1 \cdot \ldots \cdot p_k = n = q_1 \cdot \ldots \cdot q_m$, gdzie $p_1 \leqslant \ldots \leq p_k$ oraz $q_1 \leqslant \ldots \leq q_m$.

Żadna z liczb p_i nie może pojawić wśród $q_1, \ldots, q_m$ (i na odwrót), gdyż wydzielając obie strony przez p_i, otrzymalibyśmy mniejszą liczbę z dwoma różnymi rozkładami. Liczba pierwsza p_1 dzieli pierwszy iloczyn, a więc też dzieli i drugi: $p_1 | q_1 \cdot \ldots \cdot q_m$.

Zauważmy, że $p_1 \perp q_1$, gdyż są to dwie, różne liczby pierwsze. Na mocy lematu Euklidesa otrzymujemy, iż $p_1 | q_2 \cdot \ldots \cdot q_m$. Kolejno możemy wyeliminować pozostałe liczby q_i z prawego iloczynu dochodząc do $p_1 | 1$, oczywistej sprzeczności.

A oto alternatywny dowód (Eulera). Niech *n* będzie najmniejszą liczbą naturalną większą od 1 posiadającą dwa różne rozkłady na liczby pierwsze: $p_1 \cdots p_k = n = q_1 \cdots q_m$, gdzie $p_1 \leqslant \ldots \leq p_k$ oraz $q_1 \leqslant \ldots \leq q_m$.

Tak, jak poprzednio dostajemy, że żadna liczba pierwsza nie może być jednocześnie w obu rozkładach. Bez straty ogólności niech $p_1 < q_1$. Wtedy istnieje $d, r \in \mathbb{Z}$ takie, że $q_1/p_1 = d + r/p_1$, gdzie $0 < r < p_1 < q_1$ (r nie może być równe 0, gdyż oznaczałoby to iż $p_1 | q_1$). Wymnażając obie strony równości przez $q_2 \cdots q_m$ otrzymujemy $p_2 \cdots p_k = dq_2 \ldots q_m + rq_2 \ldots q_m/p_1$.

Drugi składnik w prawej stronie tej równości musi być zatem liczbą naturalną. Oznaczając ją przez x mamy więc $xp_1 = rq_2 \ldots q_m$.

Wartość obu stron powyższej równości jest mniejsza od n, gdyż $r < q_1$. Ponieważ $r < p_1$, to po rozłożeniu liczby x na czynniki pierwsze dostaniemy dwa różne rozkłady liczby mniejszej od n, co przeczy założeniu o minimalności n.

Obserwacje

Jeśli $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ jest rozkładem liczby *n* na iloczyn liczb pierwszych, to każdy jej dzielnik *d*|*n* jest postaci $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$, dla pewnych $0 \leqslant \beta_i \leqslant \alpha_i$.

Ponieważ ciągów liczb naturalnych $(\beta_1, \ldots, \beta_k)$ spełniających $0 \leqslant \beta_i \leqslant \alpha_i$ jest dokładnie $(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1)$ to mamy wniosek:

Jeśli $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ jest rozkładem liczby *n* na iloczyn liczb pierwszych, to liczba *n* ma dokładnie $(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1)$ dodatnich dzielników.

Dla trzech dowolnych liczb naturalnych jeśli *a*|*c*, *b*|*c*, $a \perp b$ to $a \cdot b | c$.

Dzięki algorytmowi Euklidesa potrafimy efektywnie znaleźć NWD dwóch liczb bez znajomości ich rozkładu.

Najmniejsza wspólna wielokrotność

Ważnym dualnym pojęciem do NWD jest pojęcie najmniejszej wspólnej wielokrotności dwu liczb, NWW.

NWW(a,b) dla dwu liczb $a, b > 0$ to najmniejsza liczba dodatnia *w* taka, że a|*w* oraz *b*|*w*.

Znając rozkłady dwu liczb możemy, analogicznie do NWD , wyznaczyć ich

$\mathrm{NWW}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdot \ldots \cdot p_k^{\max(\alpha_k,\beta_k)}$.

Wnioski:

$\mathrm{NWD}(a,b) \cdot \mathrm{NWW}(a,b) = ab.$

$\mathrm{NWW}(a,b) = \frac{a \cdot b}{\mathrm{NWD}(a,b)}$.

Twierdzenie Dirichleta (1837)

Dla dowolnych dwu dodatnich i względnie pierwszych liczb a, d istnieje nieskończenie wiele liczb pierwszych postaci $nd + a$ dla $n > 0$.

Przykład

Twierdzenie Dirichleta uogólnia wiele wcześniej znanych faktów. Dla przykładu, możemy wywnioskować, iż jest nieskończenie wiele liczb pierwszych postaci $4n + 1$ ($d = 4, a = 1$):

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$4n+1$	1	**5**	9	13	**17**	21	25	**29**	33	**37**	**41**	45	49

jak i postaci $4n + 3$ ($d = 4, a = 3$):

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$4n+3$	**3**	**7**	**11**	15	**19**	**23**	27	**31**	35	39	**43**	**47**	51

Twierdzenie Bertranda-Czebyszewa (1845, 1850)

Dla dowolnego *n*>1 istnieje liczba pierwsza *p* taka, że *n*<*p*<*2n*.

Bertrand zweryfikował poprawność swojej tezy dla liczb *n* z przedziału $[2, \ldots, 3 \cdot 10^6]$. Czebyszew przedstawił pełny dowód. W *Wykładach* mamy dowód Erdosa. Tu przedstawimy tylko lemat dotyczący funkcji zaproponowanej przez Erdosa i wykorzystanej w tymże dowodzie:

Dla $n \geq 1$ zachodzi $\vartheta(n) < n \cdot \ln 4$.

gdzie

$$\vartheta(n) = \sum_{p \in \mathbf{P}_n} \ln p,$$

oraz $\mathbb{P}_n$ oznacza zbiór liczb pierwszych nie większych od n.

$$\vartheta(n) < n \cdot \ln 4.$$

np.

ϑ(100) = $\sum$ ln *p* = ln2+ln3+ln5+ln7+ln11+ … +ln97 = 83,728...

100 x ln4 = 138,629...

Paulowi Erdos'owi udało się uogólnić Twierdzenie Bertranda-Czebyszewa na kilka sposobów. Pokazał on np., że:

- ✓ dla każdego *k* istnieje takie n_0, że dla wszystkich $n > n_0$ istnieje przynajmniej *k* liczb pierwszych większych od *n* i mniejszych od 2*n*,
- ✓ dla dowolnej liczby naturalnej *n* >6, między liczbami *n* i 2*n* znajdują się co najmniej dwie liczby pierwsze – co najmniej jedna postaci $4k + 1$ oraz co najmniej jedna postaci $4k + 3$.

Twierdzenie o liczbach pierwszych

Twierdzenie to potwierdza (i w pewnym sensie uogólnia) wszystkie obserwacje o pewnej regularności rozkładu liczb pierwszych w zbiorze liczb naturalnych.

Niech, jak poprzednio, $\mathbb{P}_n$ będzie zbiorem liczb pierwszych niewiększych od *n* oraz $\pi(n) = |\mathbb{P}_n|$. Wtedy $\pi(n) \sim n/\ln n$.

Np. π(100)=25, 100/ln100 = 100/4,6... = 21,7...

Hipotezę tę postawił Gauss, a dowód został przeprowadzony dopiero 100 lat później (w 1896). Dowód ten używa złożonych metod analitycznych, wykraczających poza ramy tego wykładu.

Twierdzenie o liczbach pierwszych opisuje asymptotyczną gęstość liczb pierwszych wśród liczb naturalnych. Z grubsza, mówi ono, iż wybierając losowo liczbę w pobliżu pewnej dużej liczby n, mamy $1/\ln n$ szansy na to, by wylosowana liczba była pierwsza.

Dla przykładu: w pobliżu n=100 mniej więcej co 5-ta liczba jest pierwsza, w pobliżu n=10 000 mniej więcej co 9-ta liczba jest pierwsza, tymczasem w pobliżu n=1 000 000 000 to już co 21-wsza liczba jest pierwsza.

A więc, statystycznie, w przedziale (n, $2n$) jest znacznie więcej liczb pierwszych niż mówią poprzednie twierdzenia. Problem polega na tym, że choć wiemy, że musi ich być bardzo dużo, to nie jesteśmy w stanie udowodnić, że dla konkretnie rozważanej liczby n nie nastąpiło jakieś "lokalne zaburzenie".

Słabe twierdzenie o liczbach pierwszych

$$\pi(n) = O(n/\ln n)$$

Dowód - szkic

Nierówność $\vartheta(n) < n \cdot \ln 4$ można wyrazić jako $\prod_{p \in \mathrm{P_n}} p < 4^n$,

a ten iloczyn jest większy lub równy $\pi(n)$!

Ze wzoru Stirlinga mamy:

$$\left(\frac{\pi(n)}{e}\right)^{\pi(n)} < (\pi(n))! < \prod_{p \in \mathbf{P}_n} p < 4^n.$$

Logarytmując stronami otrzymujemy $\pi(n) \cdot (\ln \pi(n) - 1) < n \cdot \ln 4$,
co implikuje $\pi(n) = O(n/\ln n)$.

Liczby pierwsze bliźniacze

Oprócz pary 2, 3 żadne inne liczby pierwsze nie mogą być sąsiednie (bo jedna z nich musiałaby być parzysta). Inaczej przedstawia się sprawa z dwoma kolejnymi liczbami nieparzystymi. Jeśli są one ponadto liczbami pierwszymi to nazywamy je liczbami pierwszymi bliźniaczymi.

Pierwsze takie pary to (3,5), (5,7), (11,13), (17,19), (29,31), (41,43) …

W pierwszym tysiącu liczb naturalnych takich par jest 35, i pojawiają się one coraz rzadziej.

Hipoteza: par liczb pierwszych bliźniaczych jest nieskończenie wiele.

Największa znana para takich liczb to $65\,516\,468\,355 \cdot 2^{333333} \pm 1$

Lemat: trojaczki, czyli trójka liczb pierwszych postaci (p, p+2, p+4) są wyjątkiem; jest tylko jedna taka trójka (3,5,7).

Liczby Mersenne'a

W *Cogitata Physico-Mathematica* (1644) Mersenne twierdzi, że jeśli p jest liczba pierwszą nie większą od 257, to liczba $2^p–1$ jest pierwsza wtw gdy p= 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257. Ostatnia z tych potęg ma 77 cyfr!

Łatwo policzyć, że $2^{11}–1$ nie jest pierwsza. Ale ostatnia z tych liczb ma 77 cyfr! Ostatecznie listę tych liczb zweryfikowano w 1947. Okazało się, że Mersenne pomylił się kilka razy: jego lista zawiera dwie potęgi, których nie może tam być (67, 257) i brakuje na niej trzech takich, które powinny tam wystąpić (61, 89, 107).

Jednak liczby z tej poprawionej listy, a także dalsze liczby pierwsze otrzymane według tego wzoru, nazywamy liczbami pierwszymi Mersenne'a. Używa się ich w programach komputerowych zawierających testy pierwszości. Obecnie znamy 47 takich liczb. Ostatnia ma około 13 milionów cyfr.

Małe twierdzenie Fermata (1640)

Jeśli p jest liczbą pierwszą, a jest dodatnią liczbą naturalną, $a \perp p$ to $a^{p-1}-1$ jest podzielna przez p (zatem również $p \mid a^p-a$).

Przykłady:

($3^6-3=729-3=726$ i $6 \mid 726$) ale 6 nie jest liczba pierwszą

($2^9-2=510$ i nieprawda, że $9 \mid 510$) zatem 9 nie jest liczba pierwszą

($9^3-9=729-9=720$ i prawda, że $3 \mid 720$) ale $9^2-1=80$ i nieprawda, że $3 \mid 9^2-1$

Twierdzenie to jest używane w komputerowych testach pierwszości.

Chińska wersja tego twierdzenia ($p \mid 2^p-2$) jest wcześniejsza o 2 tysiące lat, ale błędnie przyjmowała równoważność, a nie implikację!

Dowód indukcyjny Eulera (1736)

Przeprowadzamy dowód indukcyjny dla twierdzenia postaci:
Jeśli p jest liczbą pierwszą, a jest liczbą naturalną to $p \mid a^p - a$.

Zakładamy, że jest to prawda dla liczby a. Dla liczby $a+1$ możemy $(a+1)^p$ zapisać jako rozwinięcie ze wzoru dwumianowego Newtona. Następnie a^p+1^p przeniesiemy na lewą stronę. Prawa strona będzie podzielna przez p bo wszystkie składniki zawierają czynnik p (uwaga: rozpisz symbol Newtona „p po i" dla i od 1 do p-1).

Teraz do lewej strony postaci

$(a+1)^p - (a^p+1^p)$

dodamy $a^p - a$, które z założenia jest podzielne przez p.

Po prostym przekształceniu otrzymujemy $(a+1)^p - (a+1)$ …

Fałszywa hipoteza Fermata

$2^{2^n}+1$ jest liczba pierwszą

Pięć początkowych liczb tak (3, 5, 17, 65537), ale kolejna już nie:

$F_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$

Hipoteza Golbacha (1752)

Każda liczba parzysta większa od 2 może być zapisana jako suma dwóch liczb pierwszych (niekoniecznie różnych).

Euler sprawdził tę hipotezę do 2500.

Obecnie sprawdzono ją do 2 bilionów.

Po co nam liczby pierwsze?

W 1975 wymyślono algorytm szyfrowania asymetrycznego.

Pomysł polega na stosowaniu funkcji jednokierunkowych. Funkcję taką można porównać z pomieszaniem dwóch losowo wybranych puszek z różnymi farbami. Otrzymany kolor bardzo trudno rozłożyć na te dwie składowe. Teraz, zamiast farb weźmy liczby pierwsze. Jeśli otrzymany iloczyn jest mały (np. 91), to można szybko sprawdzić, że pomnożono 7 przez 13. Dla dużych liczb może być to trudniejsze.

W 1994 roku 1600 ochotników rozłożyło w Internecie liczbę o 129 cyfrach na czynniki pierwsze. Złamanie szyfru o długości 1024 cyfr zajęłoby prawie 14 miliardów lat (jest to szacowany wiek wszechświata).

Znaczne części tego wykładu pochodzą z [4]
oraz książki E. Gracjana: *Liczby pierwsze. W drodze do nieskończoności*.
Seria: Świat jest matematyczny. RBA 2012